

---

# iSecure

## Funktionsbeschreibung

---

Ein gemeinschaftlich entwickeltes Produkt der Firmen

IP-Online GmbH, Mannheim

und

SCOPE  Consulting GmbH, Mannheim

---

**Version:**

1.1

**Datum:**

24. April 2001

**Autor:**

Ralf Schiemann

Christoph Geis

**Dokument:**

iSecure-Funktionsbeschreibung.doc

**SCOPE  Consulting GmbH**  
**Willy-Brandt-Platz 6**

**D-68161 Mannheim**

**IP-Online GmbH**  
**Willy-Brandt-Platz 6**

**D-68161 Mannheim**

## Inhaltsverzeichnis:

|                                                           |    |
|-----------------------------------------------------------|----|
| Sichere Systeme in einem unsicheren Internet .....        | 3  |
| Die Lösung: .....                                         | 3  |
| Was ist iSecure.....                                      | 3  |
| Wie schützt iSecure .....                                 | 4  |
| ➤ Schutz vor Flood-Attacks (Basis): .....                 | 5  |
| ➤ Zugriffsbeschränkung auf das System (Basis): .....      | 5  |
| ➤ Beschränkte und gesicherte Serverdienste (Basis): ..... | 5  |
| ➤ Untersuchung gültiger IP-Header (Basis): .....          | 5  |
| ➤ Untersuchung des IP-Pakets (Basis):.....                | 5  |
| ➤ TCP/IP FingerPrint-Schutz (Basis): .....                | 6  |
| ➤ Einstellbare UDP-Verbindungen (Basis):.....             | 6  |
| ➤ Längenbeschränkung von ICMP-Paketen (Basis): .....      | 6  |
| ➤ „Blacklist“ (Option):.....                              | 6  |
| ➤ Paket-Level-Firewall (Option):.....                     | 6  |
| ➤ Application-Level-Firewall (Option):.....               | 7  |
| ➤ Zentrale Administration (Option):.....                  | 7  |
| Architektur .....                                         | 7  |
| Einsatz-Szenarien.....                                    | 8  |
| Kleines Netzwerkumfeld.....                               | 8  |
| Mittleres Netzwerkumfeld .....                            | 9  |
| Großes Netzwerkumfeld.....                                | 10 |
| Abkürzungsverzeichnis .....                               | 11 |

## Sichere Systeme in einem unsicheren Internet

Bieten Sie Dienste im Internet an?

Sind Ihre Server über das Internet erreichbar?

Die Anzahl der Angriffe auf Internet-Diensteanbieter ist in einem hohen Maße gestiegen. Das Ziel dieser Angriffe richtet sich fast ausschließlich auf die Verfügbarkeit der betroffenen Systeme.

Die Nichterreichbarkeit Ihrer Internet-Präsenz hat in vielen Fällen direkte Auswirkungen auf Ihren Umsatz und den Werbeeffect, den Sie im Internet erreichen wollen.

Mit den im Markt erhältlichen Hilfsmitteln können Sie nur reagieren – eine proaktive Funktionalität zur Erkennung und Abwehr solcher Angriffe auf Ihre Systeme steht Ihnen nur eingeschränkt zur Verfügung.

### Die Lösung:

**iSecure** 



### Was ist iSecure

Die (distributed) Denial of Service-Attacks (DoS, bzw. DDoS) der jüngsten Vergangenheit auf bekannte Internet-Systeme haben gezeigt, daß der Bedarf an Tools, die erfolgreich gleiche oder ähnliche Attacks verhindern können, sehr hoch ist.

IP-ONLINE und SCOPE  haben die Art und Weise dieser und anderer Angriffe auf Systeme im Internet untersucht. Das Resultat dieser Untersuchungen ist ein System, das die ein- und ausgehenden Netzwerkpakete mittels eines Regelwerkes überwacht und entsprechend behandelt (weiterleiten oder blockieren). IP-ONLINE und SCOPE  bieten ihren Kunden diese Funktionalität mit dem gemeinschaftlich entwickelten Produkt **iSecure** an.

**iSecure** bietet das Rundum-Sorglos-Paket, das Systeme vor Denial-of-Service-Attacken absichert. Die **iSecure**-Technologie schützt somit die Systeme wirksam vor destruktiven Zugriffen. Vorhandene Firewall-Systeme werden durch **iSecure** sinnvoll ergänzt oder können mit der aktivierten Firewall-Option von **iSecure** ersetzt werden.

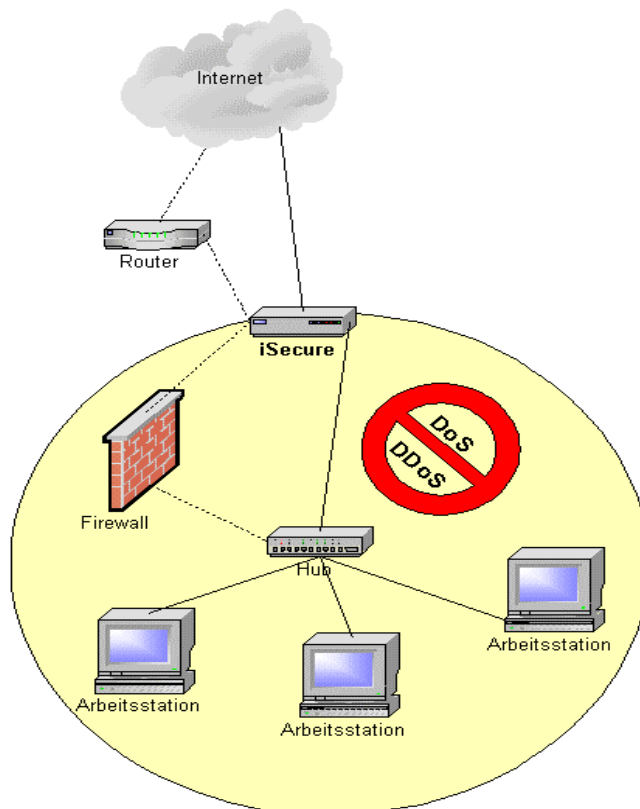
**iSecure bietet:**

- Schutz vor (Distributed) Denial-of-Service-Attacken
- Firewall-Funktionalität auf Netzwerk- oder Applikations-Ebene
- Erkennung ungültiger, bzw. fehlerhafter Netzwerkpakete
- Eine Möglichkeit zur Blockung bestimmter IP-Adressen (automatisch und manuell)
- Einen Mechanismus zum Verschleiern Ihrer Server-Betriebssysteme

**iSecure** bindet sich als kombinierte Soft-/Hardware-Lösung („Blackbox“) nahtlos in bestehende TCP/IP-Netzwerkübergänge ein. Mit Hilfe gesicherter Kanäle kann die Administration und Laufzeitbeobachtung von **iSecure** zentral durchgeführt werden.

**iSecure macht die Datenleitung intelligent.**

**Wie schützt iSecure**



**iSecure** schützt sich und die dahinter geschalteten Systeme im internen Netzwerk mittels unterschiedlicher Methoden, die aufgrund der Modularität des Produktes **iSecure**, abhängig vom Auslieferungsumfang, gesamtheitlich oder eingeschränkt zum Einsatz kommen.

**iSecure** besitzt die folgenden Systemmerkmale:

➤ **Schutz vor Flood-Attacken (Basis):**

Diese Komponente ist das „Herzstück“ von **iSecure**. Durch ein intelligentes Regelwerk werden alle durch **iSecure** geschützten Systeme vor Angriffsversuchen mittels DoS- und DDoS-Attacken abgesichert. Das gilt natürlich ebenfalls für **iSecure** selbst.

Hintergrund: DoS- und DDoS-Attacken haben zum Ziel, den oder die Zielsysteme durch eine Flut von Verbindungsaufbau-Paketen zum Erliegen zu bringen. Die angegriffenen Systeme sind anschließend nicht mehr in der Lage, auf Kommunikationsanforderungen zu reagieren.

Durch eine besondere Behandlung der eingehenden Netzwerkpakete wird sichergestellt, daß nur die legitimen Anforderungen passieren können und die Zielsysteme (wie z.B. der WWW- oder Email-Server) nicht durch Flood-Angriffe zum Erliegen kommen.

➤ **Zugriffsbeschränkung auf das System (Basis):**

Zur kontrollierten Konfiguration und Sicherstellung der uneingeschränkten Lauffähigkeit von **iSecure** sind administrative Eingriffe lediglich von der Konsole oder über gesicherte (verschlüsselte) Netzwerk-Verbindungswege möglich. Über frei einstellbare Zeitfenster kann zudem der Zugriff detaillierter eingeschränkt werden.

➤ **Beschränkte und gesicherte Serverdienste (Basis):**

Es ist sichergestellt, daß **iSecure** nur solche Dienste zur Ausführung bringt, die für die eigenen Funktionen zwingend notwendig sind. Der Zugriff auf diese Serverdienste von außen wird über einstellbare Regeln geregelt.

➤ **Untersuchung gültiger IP-Header (Basis):**

Viele TCP/IP-Implementierungen reagieren mit einem Fehlverhalten, wenn der Header eines IP-Paketes einen ungültigen Aufbau besitzt. **iSecure** überprüft den Aufbau jedes IP-Paketes auf Gültigkeit, bevor es weitergeleitet wird. Ungültige Pakete werden verworfen. Hierdurch wird sichergestellt, daß nur IP-Pakete mit korrektem Aufbau an die Zielsysteme gelangen.

➤ **Untersuchung des IP-Pakets (Basis):**

Die Gültigkeit von IP-Paketen wird anhand verschiedener Checks geprüft, bevor es zur weiteren Bearbeitung kommt. In diesem Prozeßschritt überprüft **iSecure** beispielsweise die Länge und die Prüfsumme des IP-Paketes. TCP/IP-Implementierungen verschiedener Hersteller haben in der Vergangenheit ungewollte Reaktionen gezeigt, wenn die Angaben im IP-Paket mit dem Aufbau des IP-Pakets nicht übereinstimmen.

➤ **TCP/IP FingerPrint-Schutz (Basis):**

**„Mechanismus zum Verschleiern der Server-Betriebssysteme“**

Um Angriffe auf Systeme erfolgreich durchführen zu können, ist das Wissen um das darauf laufende Betriebssystem wichtig. TCP/IP FingerPrint-Routinen (bspw. „nmap“) untersuchen das Verhalten der TCP/IP-Implementierung des Zielsystems und können daraus das Betriebssystem ableiten. **iSecure** stellt mit seiner Funktionalität sicher, daß der Angreifer durch Analyse der Antwortpakete keine Rückschlüsse auf das verwendete Betriebssystem erhält.

➤ **Einstellbare UDP-Verbindungen (Basis):**

**iSecure** sperrt standardmäßig alle UDP-Netzwerkpakete, so daß über das Netzwerkprotokoll UDP keine Angriffe auf Ihre Systeme durchgeführt werden können.

Bieten Sie jedoch Dienste an, die über UDP erreicht werden müssen (bspw. Nameserver), können Sie diese gezielt freischalten. **iSecure** wird danach Nachrichten auf explizit diese UDP-Ports weiterleiten - die übrigen Ports bleiben weiterhin geschlossen.

➤ **Längenbeschränkung von ICMP-Paketen (Basis):**

Um Rechner in einem TCP/IP-Netzwerk anzugreifen, werden unterschiedliche Methoden angewendet. Eine Möglichkeit hierzu ist das Versenden von ICMP-Nachrichten mit einer unverhältnismäßig hohen Paketlänge.

Um auch dieses Problem proaktiv zu bekämpfen, können Sie **iSecure** anweisen, solche Nachrichten entweder auf eine durch Sie festgelegte Paketlänge zu reduzieren oder sofort zu verwerfen, anstatt diese ungehindert an das Zielsystem weiterzuleiten.

➤ **„Blacklist“ (Option):**

Die Möglichkeit, bestimmte externe IP-Adressen von der Kommunikation auszuschließen, erhöht die Gesamtsicherheit der eigenen Systeme. Wird bspw. erkannt, daß von einem Rechner aus dem Internet untersucht wird, welche Ports auf den eigenen Systemen offen und damit angreifbar sind (ein sog. „Portscan“), kann **iSecure** angewiesen werden, alle Pakete von diesem Rechner zu verwerfen.

Die Liste der ausgeschlossenen Rechner kann später modifiziert werden, so daß alte Einträge wieder gelöscht werden können.

➤ **Paket-Level-Firewall (Option):**

**iSecure** kann optional zusätzlich als Paket-Level-Firewall eingesetzt werden. Hierdurch werden ein- und ausgehende IP-Pakete anhand frei definierbarer Regeln untersucht und aufgrund des Regelwerkes abgelehnt oder weitergeleitet.

Für die Erstellung der Regeln steht ein einfach zu bedienendes Administrationswerkzeug zur Verfügung, mit dem u.a. Ausschlüsse, Einschränkungen und Log-Ausgaben auf Basis bestimmter Kriterien eines IP-Paketes festgelegt werden können. Das Administrationsprogramm erstellt anschließend eine Konfigurationsdatei für die Firewall.

➤ **Application-Level-Firewall (Option):**

Zusätzlich der optionalen Firewall-Funktionalität auf IP-Paket-Ebene kann **iSecure** um Schutzmechanismen in Bezug auf die erreichbaren Dienste erweitert werden, die u.a. über die IP-Protokolle HTTP, FTP, NNTP, POP, IMAP, SMTP, X, LDAP, LPR, Socks oder SSL erreichbar sind. Der Ausschluß bestimmter Dienste oder auch Benutzer oder die Umlenkung von Dienstanfragen auf andere Server wird mit dieser Funktionalität gewährleistet.

Die einfache Konfiguration dieser Komponente wird über eine Administrationsoberfläche ermöglicht, über die solche Einschränkungen festgelegt werden können.

➤ **Zentrale Administration (Option):**

iSecure bietet die Möglichkeit die Administration bspw. spezieller ICMP-Behandlungen zentral durchzuführen. Hierzu verfügt iSecure über ein dediziertes Interface, über das der entsprechende Administrator gezielten Zugang zu der Konfigurationsumgebung erhält.

Mit diesem Framework erhält der Administrator die Möglichkeit, neben der Einstellung neuer Parameter bestimmte Laufzeitinformationen (bspw. aktueller Status, Anzahl der aktuell hergestellten Verbindungen und Anzahl der aktuell abgewiesenen Verbindungsversuche) abzufragen. Darüber hinaus wird mit Hilfe dieses Frameworks die Verteilung bestimmter Informationen, z.B. Blacklist-Einträge, auf alle angeschlossenen iSecure-Systeme sichergestellt.

## Architektur

**iSecure** ist eine kombinierte Hard- und Softwarelösung („Blackbox“), die sowohl in kleinen, mittleren und großen Netzwerkumgebungen eingesetzt werden kann.

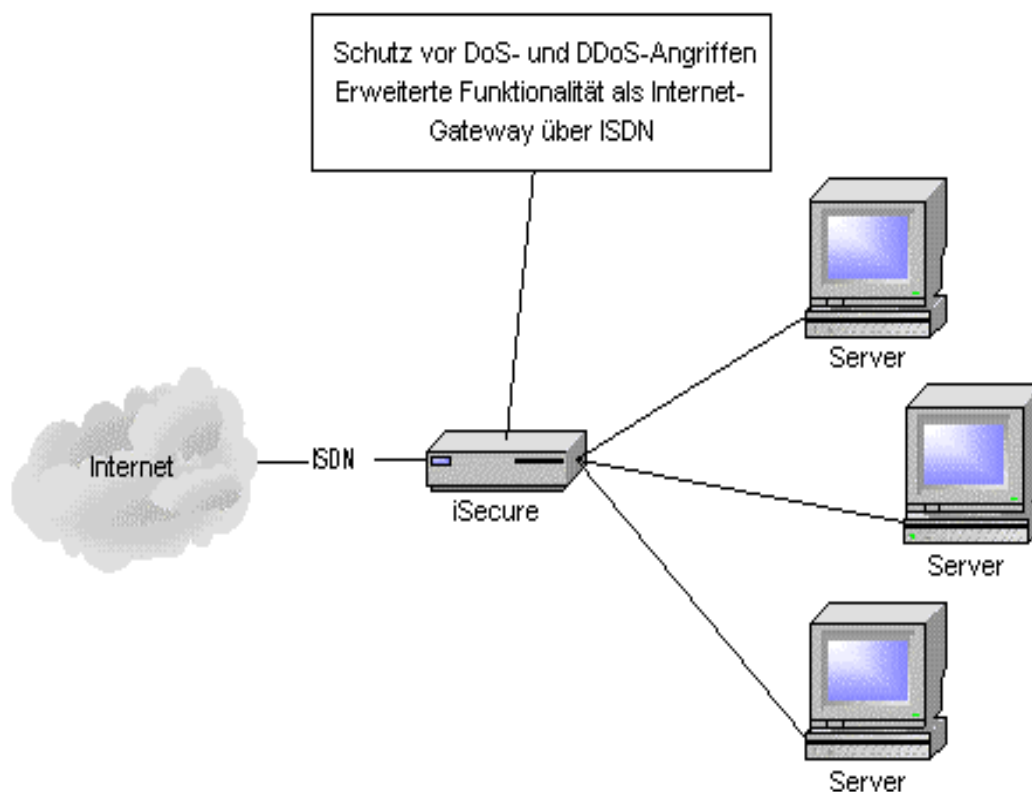
Die **iSecure**-Hardware wird standardmäßig mit zwei 100Mbit Ethernet-Netzwerkkarten ausgeliefert. Die Standardkonfiguration kann jedoch auf die jeweilige Infrastruktur angepaßt werden, z.B.:

- 1 Ethernet- und 1 ISDN-Adapter,
- 1 Token-Ring- und 1 ISDN-Adapter oder,
- 1 Token-Ring und 1 Ethernet-Adapter.

## Einsatz-Szenarien

Dieser Abschnitt zeigt die typischen Einsatzgebiete von **iSecure** in kleinen, mittleren und großen Netzwerken. Die Grafiken sind beispielhafter Natur und sollen lediglich die Funktionalität von **iSecure** aufzeigen.

### Kleines Netzwerkumfeld

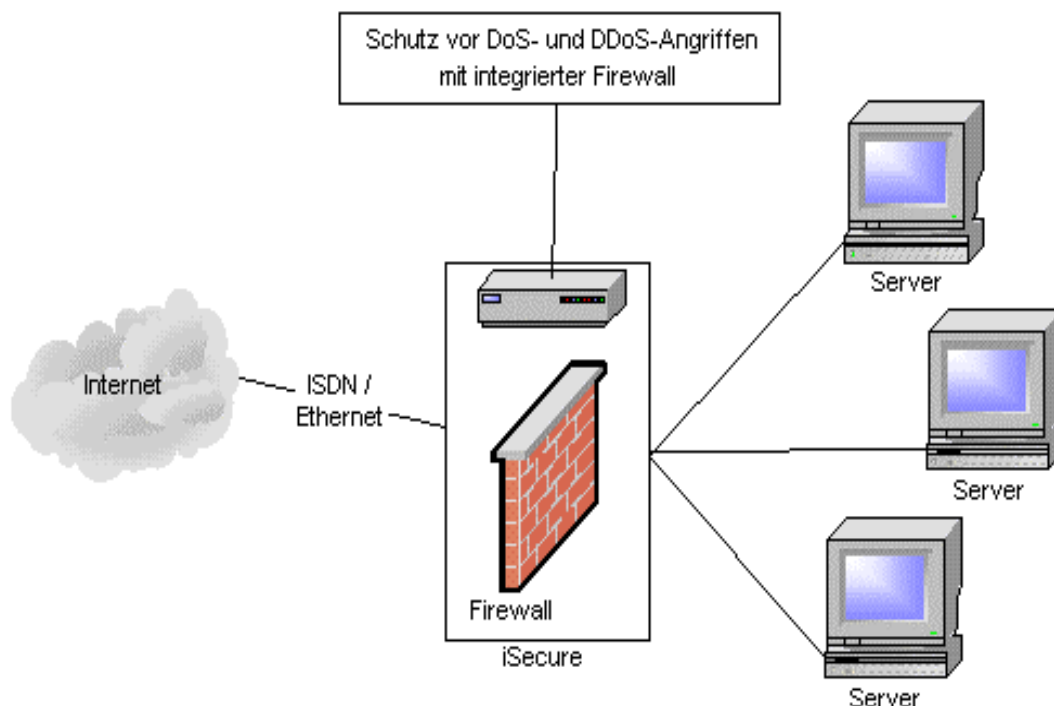


Diese Grafik zeigt den Einsatz von **iSecure** in einem kleinen Netzwerk. Hier ist die Hardware mit einem Ethernet- und einem ISDN-Adapter ausgestattet.

Neben dem Schutz der im LAN liegenden Systeme vor DoS-Attacken wird in diesem Beispiel **iSecure** als Router für den Zugriff auf Dienste des Internets verwendet. Der ISDN-Verbindungsaufbau erfolgt standardmäßig immer dann, wenn eine Kommunikationsanbindung an das externe Netzwerk gewünscht ist („on demand“). Der Verbindungsabbau erfolgt automatisch, wenn **iSecure** nach einer definierten Zeitspanne keine weiteren Netzwerkpakete weiterleitet. Dieses Standardverhalten kann jedoch per Konfiguration geändert werden.

Obwohl in diesem Beispiel keine Firewall-Funktionalitäten von **iSecure** durchgeführt werden, ist dies durch Erweiterung zu jeder Zeit möglich.

## Mittleres Netzwerkumfeld



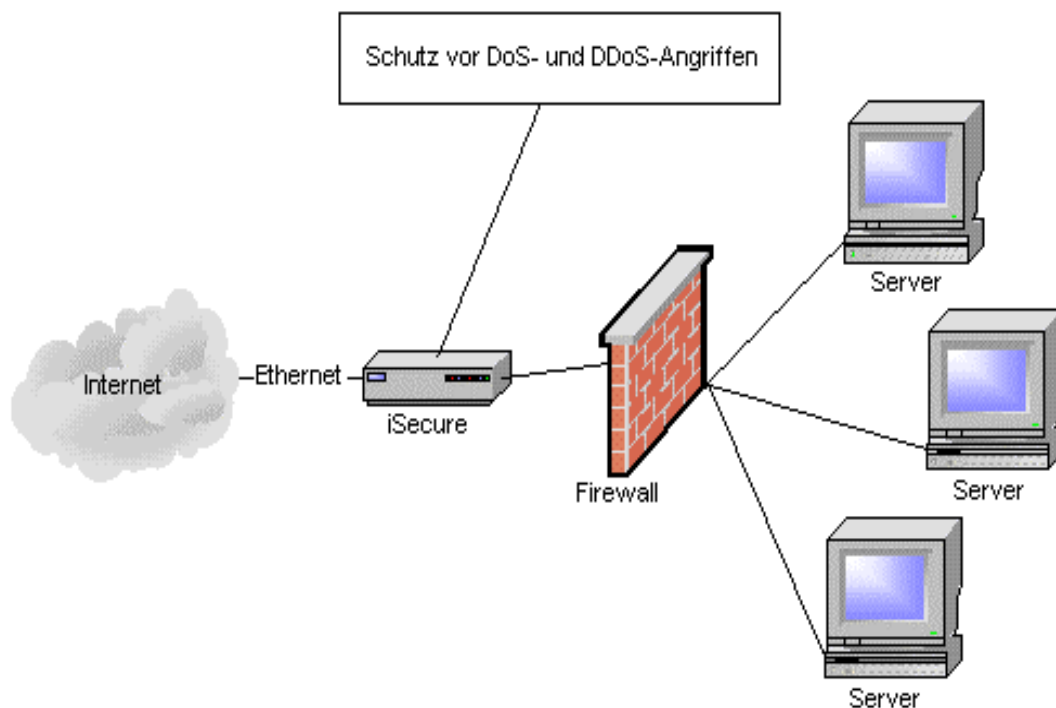
In diesem beispielhaften Netzwerkumfeld wird **iSecure** als integrierter „Firewall-Router“ eingesetzt. Die Verbindung in das externe Netz (z.B. Internet) erfolgt über **iSecure** oder über einen weiteren, dedizierten Router (nicht eingezeichnet).

Dieses Beispiel zeigt die hohe Funktionalität von **iSecure**, da hier das gesamte Leistungsspektrum genutzt wird:

- Die Server und Arbeitsplatzrechner des internen Netzwerkes nutzen **iSecure** als Übergang in das Internet (über Ethernet oder ISDN).
- **iSecure** schützt die internen Systeme vor DoS-Attacken.
- Ein- und ausgehende IP-Pakete werden anhand definierter Regeln weitergeleitet oder verworfen.
- Der Zugriff auf die öffentlich zugänglichen Dienste auf den lokalen Systemen wird anhand definierter Regeln erlaubt oder abgewiesen.

Die für die einzelnen Funktionen notwendigen Regelwerke werden über ein Konfigurationsprogramm erstellt und modifiziert, das aus den vereinfachten Benutzereingaben ein vom System lesbares Konfigurationsset erstellt. Die von **iSecure** angebotenen Funktionen sind weitestgehend frei konfigurierbar und können somit für den Einsatz in das eigene Netzwerk optimal eingestellt werden.

## Großes Netzwerkkumfeld



Obwohl in „großen“ Netzwerkkumgebungen für den Übergang in fremde Netze, wie das Internet bereits im umfassenden Maße dedizierte Router und Firewall-Systeme zum Einsatz kommen, schützen diese Systeme nicht ausreichend vor DoS-Angriffen, so daß die durch die Firewall(s) geschützten Systeme immer noch in einem hohen Maße angreifbar sind und im schlimmsten Falle nach einer erfolgreich durchgeführten Attacke ihren Dienst einstellen.

In diesem Umfeld bietet **iSecure** mit seiner Kernkompetenz den notwendigen Schutz vor solchen Flood-Angriffen. Nur Pakete, die erkennbar nicht dem Schaden der betroffenen Zielsysteme dienen, werden an die (in diesem Beispiel) dahinterliegende Firewall zur weiteren Bearbeitung geleitet. Auf der Firewall wird anschließend entschieden, ob die Netzwerkpakete weitergeleitet oder abgewiesen werden.

## Abkürzungsverzeichnis

- DDoS      Distributed Denial of Service
- DoS      Denial of Service
- FTP      File Transfer Protocol
- HTTP      Hypertext Transfer Protocol
- IMAP      Internet Message Access Protocol
- IP      Internet Protocol
- LDAP      Lightweight Directory Access Protocol
- LPR      Line Printer
- NNTP      Network News Transfer Protocol
- POP      Post Office Protocol
- SMTP      Simple Mail Transfer Protocol
- SSL      Secure Socket Layer
- WWW      World Wide Web
- X      X-Windows-System